

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-286836
(P2000-286836A)

(43)公開日 平成12年10月13日(2000.10.13)

(51) Int.Cl. ⁷	識別記号	F I	マークオフ(参考)
H 0 4 L	9/32	H 0 4 L	9/00
G 0 6 T	1/00	G 0 9 C	1/00
G 0 9 C	1/00	6 4 0	6 4 0 A
			5 J 1 0 4
		H 0 4 N	1/387
H 0 4 N	1/387	G 0 6 F	15/66
			B

審査請求 未請求 請求項の数 6 OL (全 8 頁)

(21)出願番号 特願平11-88233

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(22)出願日 平成11年3月30日(1999.3.30)

(72) 発明者 秋山 良太

神奈川県川崎市中原区上
1号 富士通株式会社内

(72) 発明者 小谷 誠剛

神奈川県川崎市中原区上
1号 富士通株式会社内

(74)代理人 100089141

參理士 署田 守弘

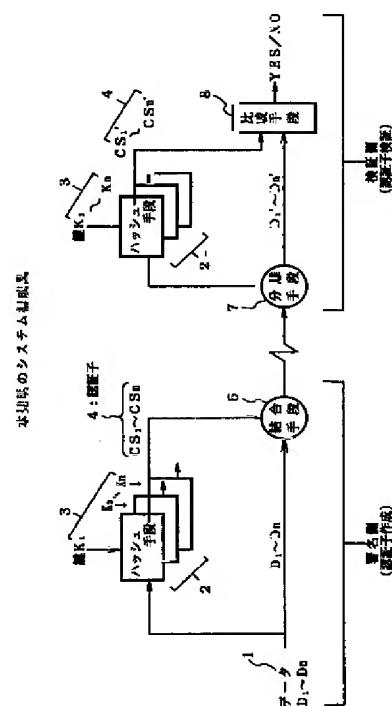
最終百に統ぐ

(54) 【発明の名称】 認証装置および記録媒体

(57) 【要約】

【課題】本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関し、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合などし、偽造情報作成確率を低減することを目的とする。

【解決手段】 情報を複数のデータに分割する手段と、分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、作成したそれぞれの認証子を情報に結合する手段とを備えるように構成する。



【特許請求の範囲】

【請求項1】情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、情報を複数のデータに分割する手段と、上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。

【請求項2】情報を鍵を用いて一方向性の関数で認証子を作成して署名する認証装置において、情報を複数のデータに分割する手段と、上記分割した1つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、上記作成したそれぞれの認証子を上記情報に結合する手段とを備えたことを特徴とする認証装置。

【請求項3】情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、情報からデータと認証子を分離する手段と、上記分離した情報を複数のデータに分割する手段と、上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、上記作成したそれぞれの認証子および上記分離したそれぞれの認証子をもとに検証する手段とを備えたことを特徴とする認証装置。

【請求項4】情報を鍵を用いて一方向性の関数で認証子を作成して検証する認証装置において、情報からデータと認証子を分離する手段と、上記分離した情報を複数のデータに分割する手段と、上記分割した1つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成することを繰り返す手段と、上記作成したそれぞれの認証子および上記分離した認証子をもとに検証する手段とを備えたことを特徴とする認証装置。

【請求項5】情報を複数に分割する手段と、上記分割した各データについてそれぞれの鍵を用いて一方向性の関数でそれぞれの認証子を作成する手段と、上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【請求項6】情報を複数に分割する手段と、上記分割した1つのデータについて鍵を用いて一方向性の関数で認証子を作成および当該一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵を用いて一方向性の関数で認証子を作成すること

を繰り返す手段と、

上記作成したそれぞれの認証子を上記情報に結合する手段として機能させるプログラムを記録したコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報を鍵を用いて一方向性の関数で認証子を作成して署名および検証する認証装置および記録媒体に関するものである。

【0002】

【従来の技術】従来、文字、数字、記号列で作成される文書（ドキュメント）の偽造を防止するために、当該文書を所定ブロックに分割して一方向性の関数（例えばハッシュ関数）を用いて認証子を作成し、文書中の数字を他の数字に変更するというような、偽造を防止するようになっていた。

【0003】

【発明が解決しようとする課題】しかしながら、上述した従来の一方向性の例えばハッシュ関数を用いて認証子を作成するシステムでは、偽造をより困難にするにはハッシュ関数の処理ブロック長を長くする手法が用いられていたが、十分な偽造が防止し得ないという問題があった。即ち、従来のハッシュ関数では、AND論理、OR論理の他四則演算子等を複雑に組み合わせて一方向性関数を実現していたが、これは経験的・直感的手法に基づいて行われ、組織的な構成法によらない。このため、従来のハッシュ関数の中には、正当なデータをハッシュ処理して得た署名データ（認証子）を不当データに改ざんして同様にハッシュ処理した結果が一致するいわゆる署名偽造が起こる問題があった。

【0004】本発明は、これらの問題を解決するため、情報を複数に分割して異なる鍵を用い任意の信頼できる一方向性関数でそれぞれ認証子を作成して結合し、偽造情報作成確率を低減することを目的としている。

【0005】

【課題を解決するための手段】図1を参照して課題を解決するための手段を説明する。図1において、ハッシュ手段2は、鍵を用いて一方向性の関数で認証子を作成するものである。

【0006】結合手段5は、認証子とデータを結合するものである。分離手段7は、情報からデータと認証子とを分離するものである。比較手段8は、情報から分離した認証子と、情報から作成した認証子とを比較するものである。

【0007】次に、動作を説明する。ハッシュ手段2が情報から分割した各データについてそれぞれの鍵3を用いて一方向性の関数でそれぞれの認証子を作成し、結合手段5が作成したそれぞれの認証子を情報に結合するようしている。

【0008】また、ハッシュ手段2が情報から分割した

1つのデータについて鍵3を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子を作成する際の中間の任意のデータと次のデータについて鍵3を用いて一方向性の関数で認証子を作成することを繰り返し、結合手段5が作成したそれぞれの認証子を情報に結合するようにしている。

【0009】また、分離手段7が情報からデータと認証子を分離し、ハッシュ手段2が分離された情報を複数に分割した各データについてそれぞれの鍵3を用いて一方向性の関数でそれぞれの認証子を作成し、比較手段8が作成したそれぞれの認証子および分離したそれぞれの認証子をもとに検証するようにしている。

【0010】また、分離手段7が情報からデータと認証子を分離し、分離された情報を複数に分割した1つのデータについて鍵3を用いて一方向性の関数で認証子を作成および一方向性の関数で認証子4を作成する際の中間の任意のデータと次のデータについて鍵3用いて一方向性の関数で認証子作成することを繰り返し、比較手段8が作成したそれぞれの認証子および分離した認証子をもとに検証するようにしている。

【0011】従って、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりすることにより、偽造情報作成確率を低減することが可能となる。

【0012】

【実施例】次に、図1から図6を用いて本発明の実施の形態および動作を順次詳細に説明する。ここでは、以下、情報（テキスト、画像（静止画、動画）、音声などからなる情報）中の文（テキスト）を例に具体的に説明する（以下の具体的な説明は、例であって、画像（静止画、動画）、音声などの全てについて同様に適用できるものである）。

【0013】図1は、本発明のシステム構成図を示す。図1において、署名側は、左側の半分によって構成され、認証子を作成して文に結合するものである。

【0014】検証側は、右側の半分によって構成され、文から認証子を分離して文から作成した認証子とを比較して検証するものである。データ1は、文から分割したデータD1ないしDnであって、後述する図5の文（ドキュメント）中の数字、文字、記号などを所定ブロック毎に分割したデータD1からDnである。

【0015】ハッシュ手段2は、データD1ないしDnについてそれぞれの鍵K1からKmを用いて一方向性の関数でそれぞれの認証子CS1からCSmをそれぞれ作成するものである。

【0016】鍵3は、認証子CS1からCSmを作成するそれぞれの鍵である。認証子4は、鍵K1からKmによって作成されたそれぞれの認証子である。結合手段5

は、作成した認証子4と、データD1からDnとを結合するものであって、後述する図5のドキュメント例に示すように、認証子4を下段に付加などするものである。

【0017】分離手段7は、文からデータD1'からDn'、および認証子4を分離するものである。比較手段8は、文から分離した認証子と、文から作成した認証子とを比較し、例えば一致したときに文が偽造されていなく真正と認証するものである。

【0018】次に、図1の構成の動作を説明する。

(1) 署名側における認証子の作成：

(1-1) 文を複数に分割した入力データD1からDn毎に、それぞれの鍵を用いてハッシュ手段2が認証子4であるCS1からCSmを作成する。

【0019】(1-2) 作成されたCS1からCSmと、データD1からDnとを結合する。例えば後述する図5のドキュメント（文）に示すように、文章中の下段に認証子（例えば1桁4ビットからなる8桁分の認証子）を付加する。

【0020】以上によって、文を分割したデータD1からDn毎にそれぞれの鍵を用いて認証子CS1からCSmを作成し、データD1からDnに結合することにより、文を分割したデータD1からDn毎に異なる鍵を用いて認証子を作成することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。

【0021】(2) 検証側における認証子の作成：

(2-1) (1)で作成された図5の文（ドキュメント）から認証子CS1からCSmとデータD1'からDn'を分離する。

【0022】(2-2) 分離したデータD1'からDn'毎に、それぞれの鍵を用いてハッシュ手段2が認証子4であるCS1'からCSm'を作成する。

(2-2) 作成されたCS1'からCSm'と、分離された認証子CS1からCSmとを比較し、一致するか判別し、一致したときに真正の文であって偽造されていないと判定する。一方、1つでも一致しないときは偽造された文と判定する。

【0023】以上によって、文から分離したデータD1からDn毎にそれぞれの鍵を用いて認証子CS1'からCSm'を作成し、分離した認証子CS1からCSmとを比較して全て一致したときに真正の文と判定し、1つでも不一致のときに偽造された文と判定することにより、文を分割したデータD1からDnについて異なる複数の鍵を用いて認証子をそれぞれ作成して結合することで偽造文の作成を極めて困難にし信頼性を大幅に向上させることが可能となる。以下順次詳細に説明する。

【0024】図2は、本発明の1実施例構成図（独立多並列）を示す。これは、文を分割した入力データD1からDnについて、m並列にそれぞれの鍵を用いてハッシュ手段2により認証子CS1からCSmを並列に同時に作成するときの構成を示す。

【0025】図2の(a)は、構成図を示す。図2の(a)において、入力データD1からDnは、文を分割したデータD1からDnである。

【0026】ハッシュ手段2は、鍵Kを用いて認証子CSを作成するものであって、ここでは、EOR21、一方向性関数(例えばハッシュ関数)22およびトランケート23から構成されるものである(図3の(b)を用いて後述する)。

【0027】EOR21は、排他論理演算を実行するものであって、ここでは、データと前回の一方向性関数22で求めた値(初回は初期値IV)との排他論理演算を行うものである。

【0028】一方向性関数(一方向性関数器)22は、鍵Kをもとに、EOR21によって演算したデータから一方向性関数(例えばハッシュ関数)によって不可逆性の認証子CSを作成するものである。

【0029】トランケート23は、一方向性関数22によって作成された認証子CSを出力するものである。出力データ(D1からDn, CS1からCSm)は、入力データD1からDnについて作成した認証子CS1からCSmを結合したものである(図5参照)。

【0030】図2の(b)は、認証子CSの生成プロセスを示す。図2の(b-1)は、CS1の生成プロセスを示す。図2の(b-1)において、

① IV=公開定数:これは、図2の(a)の左側から1番目のハッシュ手段2を構成するEOR21に初期値IVを設定する。

【0031】② EK1[IV(+D1)=L11:これは、図2の(a)のEOR21が①で設定した初期値IVと、1番目のデータD1とを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L11を得る。

【0032】③ EK1[L11(+D2)=L12:これは、図2の(a)のEOR21が②で得た値L11と、2番目のデータD2とを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L12を得る。

【0033】④ EK1[L1(n-1)(+Dn)=L1n:これは、同様にして、図2の(a)のEOR21が前回に得た値L1(n-1)と、n番目のデータDnとを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L1nを得る。

【0034】⑤ Tr[L1n]=CS1:これは、最後のn番目のデータDnまで終了したので、最後のn番目の演算結果L1nを認証子CS1として出力する。以上の①から⑤の手順によって、鍵K1、初期値IVを用いて

認証子CS1を作成することが可能となる。

【0035】図2の(b-2)、(b-3)は、図2の(b-1)の②から⑤の手順と同様に、認証子CS2, CS3を求める様子を示す。これを続けて認証子CSmを同様に求める。

【0036】以上のように、独立にm並列で鍵K1からKmをそれぞれ用いて同時に認証子CS1からCSmを算出することが可能となる。ここでは、CSm個あたりの偽造確率=1/2^{mp}(Pは認証子のビット長)となり、認証子CSの数を増やすことで偽造確率を小さくすることができると共に、並列処理ができCSの数に依存しないで同一時間で処理可能となる。

【0037】次に、図3を用いて図2のm=3(独立3並列)の場合の構成と動作を詳細に説明する。図3は、本発明の具体例構成図(独立3並列)を示す。

【0038】図3の(a)は、独立3並列の構成図を示す。これは、図2において、m=3とした場合の例であって、ハッシュ手段2、EOR21、一方向性関数22、およびトランケート23は、図2の同一番号のものと同じであるので、説明を省略する。

【0039】図3の(b)は、ハッシュ手段2におけるCS1からCS3の生成プロセスを示す。図3の(b-1)は、図3の(a)の入力データD1からDn、鍵K1、初期値IVをもとに認証子CS1を作成するときの手順を示す。

【0040】図3の(b-1)において、
① IV=公開定数:これは、図3の(a)の左側から1番目のハッシュ手段2を構成するEOR21に初期値IVを設定する。

【0041】② EK1[IV(+D1)=L11:これは、図3の(a)のEOR21が①で設定した初期値IVと、1番目のデータD1とを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L11を得る。

【0042】③ EK1[L11(+D2)=L12:これは、図3の(a)のEOR21が②で得た値L11と、2番目のデータD2とを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L12を得る。

【0043】④ EK1[L1(n-1)(+Dn)=L1n:これは、同様にして、図3の(a)のEOR21が前回に得た値L1(n-1)と、n番目のデータDnとを排他論理演算し、その排他論理演算した値について、一方向性関数22が鍵K1を用いて一方向性の演算(例えばハッシュ関数によって演算)して値L1nを得る。

【0044】⑤ Tr[L1n]=CS1:これは、最後のn番目のデータDnまで終了したので、最後のn番目

の演算結果 $L_1 n$ を認証子 $C S 1$ として出力する。図3の(b-2)、(b-3)は、図3の(b-1)の \oplus' から \oplus' の手順と同様に、認証子 $C S 2$ 、 $C S 3$ を求める様子を示す。

【0045】以上の \oplus' から \oplus' の手順によって、独立に m 並列で鍵 K_1 から K_3 をそれぞれ用いて同時に認証子 $C S 1$ から $C S 3$ を算出することが可能となる。次に、図4を用いて $m=3$ で前段の中間データを次段の初期値とする場合の構成と動作を詳細に説明する。

【0046】図4は、本発明の他の具体例構成図 ($m=3$) を示す。図4の(a)は、 $m=3$ の構成図を示す。これは $m=3$ として前段の中間データを次段の初期値とした場合の例であって、ハッシュ手段2、E OR 21、一方向性関数22、およびトランケート23は、図2の同一番号のものと同じ（初期値のみことなる）であるので、説明を省略する。

【0047】図4の(b)は、ハッシュ手段2における $C S 1$ から $C S 3$ の生成プロセスを示す。図4の(b-1)は、図4の(a)の左から1番目のハッシュ手段2で $C S 1$ を求める手順を示す。ここでは、既述した図3の(b-1)の \oplus' から \oplus' と同様にして $C S 1$ を求める。

【0048】図4の(b-2)は、図4の(a)の左から2番目のハッシュ手段2で $C S 2$ を求める手順を示す。ここでは、前段の \oplus に示す中間結果 ($L_1 (n-1)$) を初期値とし、既述した図3の(b-1)の \oplus' から \oplus' と同様にして $C S 2$ を求める。

【0049】図4の(b-3)は、図4の(a)の左から3番目のハッシュ手段2で $C S 3$ を求める手順を示す。ここでは、前段の \oplus に示す中間結果 ($L_2 (n-1)$) を初期値とし、既述した図3の(b-1)の \oplus' から \oplus' と同様にして $C S 3$ を求める。

【0050】以上の手順によって、 $m=3$ で鍵 K_1 から K_3 をそれぞれ用いて前段の中間結果を次段の初期値として認証子 $C S 1$ から $C S 3$ を順次算出し、より信頼性を向上させることが可能となる。

【0051】図5は、本発明の文の例を示す。ここでは、文（ドキュメント）は、例えば図示のように、文字、数字、記号などから構成され、これらを任意数毎にブロックに分割してデータ D_1 から D_n を作成している。また、データ D_1 から D_n よりそれぞれの鍵 K_1 から K_m で作成した認証子 $C S 1$ から $C S_m$ を結合してドキュメントの下段の特定位置に8桁（1桁4ビット）の認証子列を附加している。

【0052】図6は、概念説明図を示す。図6の(a)は本発明の概念説明図を示し、図6の(b)は従来技術の概念説明図を示す。

【0053】図6の(b)において、文空間 M は偽造対象の文の取りうる仮想的な空間であり、認証子空間は認証子の取りうる仮想的な空間である。文空間 M 上で偽造をより防止するには、従来では、図示のように、認証子を長ブロックにして偽造確率を小さくしていた（認証子空間上で同じ値となる、文空間 M 上での偽造文空間 M_2 を点線から実線の円に示すように小さくしていた）。

【0054】図6の(a)において、鍵 K_1 を用いた場合の文空間 M 上での偽造文空間 M_1 、鍵 K_2 を用いた場合の文空間 M 上での偽造文空間 M_2 、鍵 K_3 を用いた場合の文空間 M 上での偽造文空間 M_3 とすれば、本発明における鍵 K_1 、 K_2 、 K_3 の3つを用いた場合には、偽造空間 M_1 、 M_2 、 M_3 の共通領域である非常に小さな偽造空間 M_{123} となり、偽造確率を大幅に小さくすることが可能となる。

【0055】

【発明の効果】以上説明したように、本発明によれば、情報を複数に分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して結合したり、情報から分離した認証子と情報から分離したデータを分割して異なる鍵を用いて一方向性関数でそれぞれ認証子を作成して検証したりする構成を採用しているため、偽造情報作成確率を簡易な手法で低減できると共に、並列処理により認証子作成時間を増やすことなく偽造情報確率を小さくしたり、前段の認証子作成時の任意の中間データを次段の初期値などとして使用することで更に偽造確率を小さくしたりできる。

【図面の簡単な説明】

【図1】本発明のシステム構成図である。

【図2】本発明の1実施例構成図（独立多並列）である。

【図3】本発明の具体例構成図（独立3並列）である。

【図4】本発明の多の具体例構成図 ($m=3$) である。

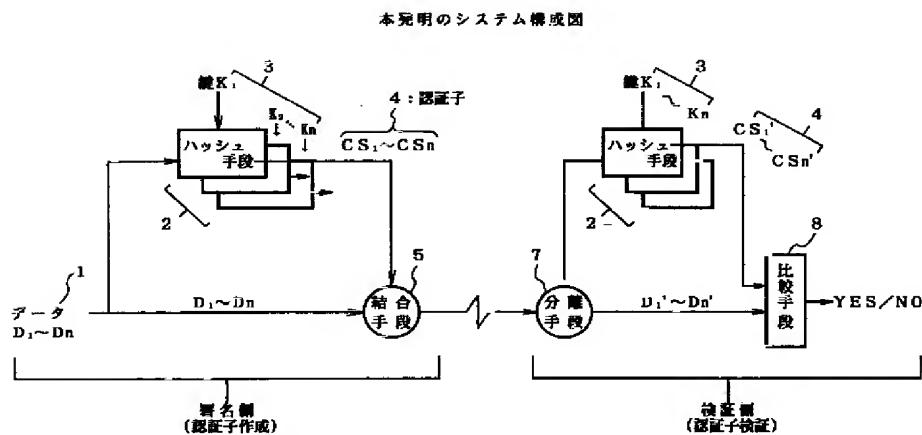
【図5】本発明の文の例である。

【図6】概念説明図である。

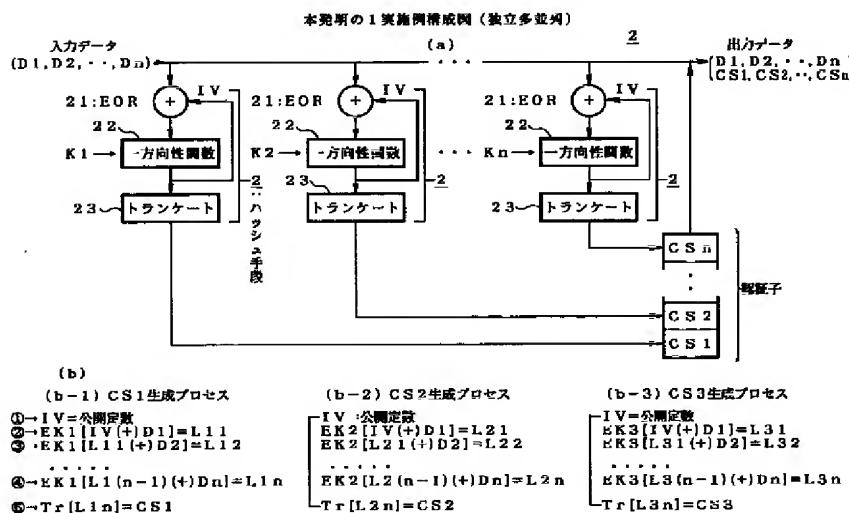
【符号の説明】

- 1 : データ
- 2 : ハッシュ手段
- 3 : 鍵
- 4 : 認証子
- 5 : 結合手段
- 7 : 分離手段
- 8 : 比較手段
- 21 : E OR (排他論理和演算器)
- 22 : 一方向性関数器
- 23 : トランケート

【図1】

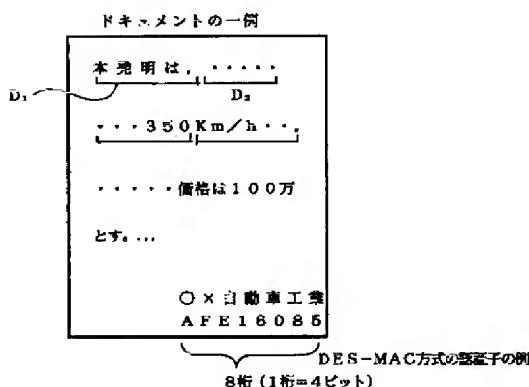


【図2】

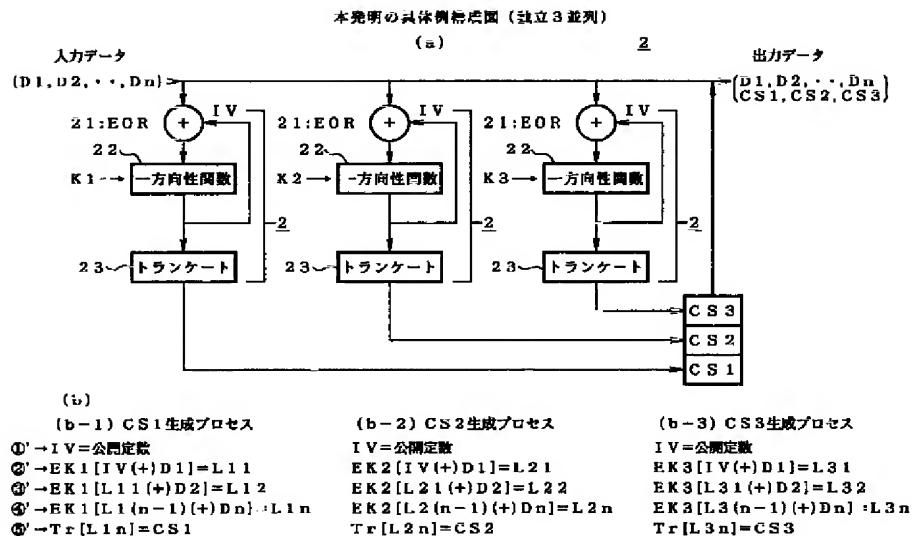


【図5】

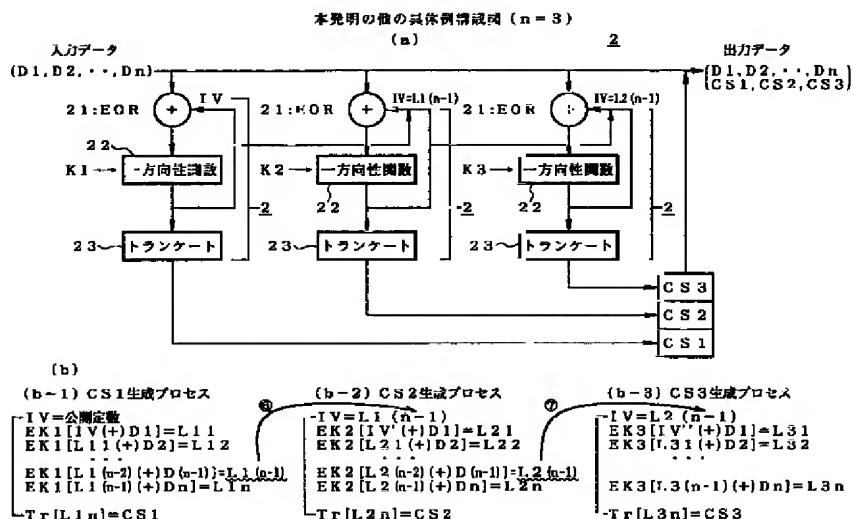
本発明の文の例



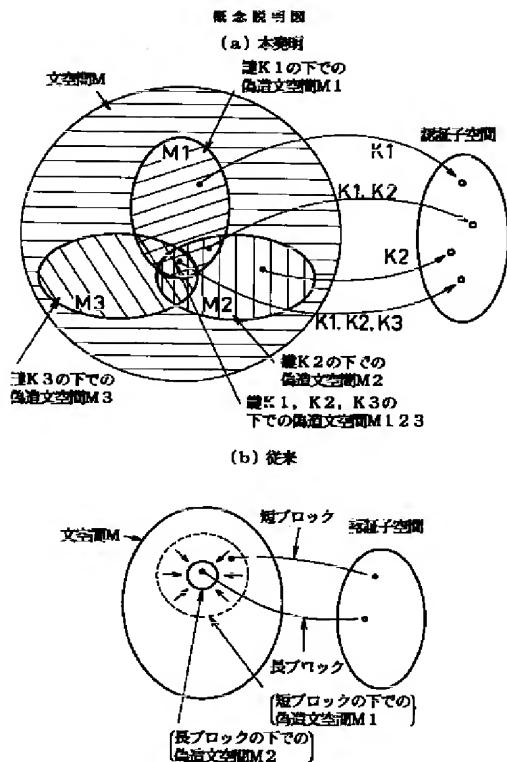
【図3】



【図4】



【図6】



フロントページの続き

(72)発明者 長谷部 高行
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72)発明者 佐々木 孝興
東京都港区芝浦四丁目15番33号 株式会社
富士通ビー・エス・シー内

F ターム(参考) 5B057 CA12 CA16 CB12 CB16 CC02
CE08 CG07 CH08
5C076 AA14 AA36 AA40 BA06
5J104 AA08 JA03 LA01 LA02 LA05
LA06 NA02 NA11